Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1-15 (Cancelled)

16. (Previously Presented) A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network via a Security Gateway, the method comprising the steps of:

(1) negotiating at least one Security Association between the mobile host and a correspondent host of a Virtual Private Network ;

(2) initiating a communication between the mobile host and the Security Gateway and sending an authentication certificate to the Security Gateway, the certificate including data identifying a Security Association which will be used for subsequent communication between the mobile host and the correspondent host; and

(3) sending data packets from the mobile host to the correspondent host using the identified Security Association, via the Security Gateway;

wherein said data packets are forwarded by the Security Gateway to the correspondent host only if they are authenticated by the Security Gateway.

17. (Previously Presented) The method according to claim 16, comprising the additional steps, prior to step (2), of negotiating at least one Security Association between the mobile host and the Security Gateway and sending said authentication certificate to the Security Gateway using one of the at least one Security Associations between the mobile host and the Security Gateway.

18. (Previously Presented) The method according to claim 16, wherein said authentication certificate comprises data indicating an IP address of the mobile host.

19. (Previously Presented) The method according to claim 16, wherein said at least one Security Association is an IPsec phase 2 Security Association and is used on top of an Internet Security Association Key Management Protocol Security Association.

20. (Previously Presented) The method according to claim 19, wherein said authentication certificate contains Internet Security Association Key Management Protocol cookies of the mobile host and said correspondent host with which the phase 2 negotiation was done.

21. (Previously Presented) The method according to claim 16, wherein the Security Gateway is coupled between the intranet and a core network of a mobile wireless telecommunications system.

22. (Previously Presented) The method according to claim 16, wherein the mobile host is a wireless host coupled to the Security Gateway via an access network.

23. (Previously Presented) The method according to claim 16, wherein the Virtual Private Network comprises an intranet, with the Security Gateway being coupled between the intranet and the Internet.

24. (Previously Presented) The method according to claim 23, wherein said correspondent host resides within the intranet and said data packets are forwarded to the correspondent host from the Security Gateway over a secure connection.

25. (Previously Presented) The method according to claim 16, wherein a negotiated Security Association expires after a predefined volume of data has been sent using the Security Association.

26. (Previously Presented) The method according to claim 16, wherein a negotiated Security Association is time limited by the Security Gateway and, after a predefined time limit, the Security Association is suspended by the Security Gateway.

27. (Previously Presented) The method according to claim 16, wherein the data packets sent in step (3) and which contain user data are authenticated by the Security Gateway using authentication data sent in separate data packets.

28. (Previously Presented) The method according to claim 17, wherein the data packets sent in step (3) and which contain user data are authenticated by the Security Gateway using authentication data sent in separate data packets, and wherein the data packets containing user data are sent using a Security Association negotiated between the mobile host and said correspondent host and the data packets containing authentication data are sent using a Security Association negotiated between the mobile host and the Security Gateway.

29. (Previously Presented) A Security Gateway of a Virtual Private Network, the Security Gateway enabling secure communication between a mobile host and a correspondent host, the Security Gateway comprising:

(1) means for negotiating one or more Security Associations between the mobile host and the Security Gateway ;

(2) means for subsequently initiating a communication between the mobile host and the Security Gateway using a negotiated Security Association and for receiving an authentication certificate sent from the mobile host, the certificate including data identifying the mobile host and an IP address of the mobile host;

(3) means for receiving data packets sent from the mobile host and for authenticating the data packets; and

(4) means for forwarding the data packets from the Security Gateway to said correspondent host only if the received data packets are authenticated.

30. (Previously Presented) A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network, the method comprising the steps of:

(1) negotiating one or more Security Associations between the mobile host and a Security Gateway of a Virtual Private Network ;

(2) initiating a communication between the mobile host and the Security Gateway using a negotiated Security Association and sending an authentication certificate to the Security Gateway, the certificate including data identifying the mobile host and an IP address of the mobile host;

(3) sending data packets from the mobile host to the Security Gateway and authenticating the data packets at the Security Gateway; and

(4) forwarding the data packets from the Security Gateway to said correspondent host only if the received data packets are authenticated.